가상화 환경과 리눅스 시스템 공격 증가
크로스 플랫폼 언어 활용, RaaS 기반 랜섬웨어 등장으로 전술 변화

해외 주요 랜섬웨어 공격 동향과 2025년 전망

요약

1. 주요 10대 랜섬웨어, 전체 피해량 53% 차지

- 2024년 피해건수 5,943건 (전년도 대비 11.37% 증가)
- 가상화 환경과 리눅스 시스템을 노린 공격 증가 및 이를 활용한 새로운 공격 그룹 등장

2. 주요 피해 산업

- 디지털 의존도, 데이터 시장성, 보안 취약성 특징을 가진
  기술, 헬스케어, 제조업이 주요 공격 대상
- 의료기관 대상 공격 증가
  1) 미국 최대 의료 청구 처리업체 “Capital Health”**(7TB 의료 데이터 탈취)**
  2) 의료 비영리 단체 “Planned Parenthood” **(금융 정보, 법원 서류, 보험 증서 유출)**

3. 공격 특이점

- 가상화 환경과 리눅스 시스템 공격: 1) VMware ESXi 서버 표적 공격
  2) 새로운 리눅스 변종을 통한 서버 환경 위협
- 엔드포인트 탐지 소프트웨어를 무력화하는 EDR Killer BYOVD 공격 사례 급증

4. 2025년 공격 전망

- 크로스 플랫폼 언어를 활용한 공격기법 확대, 피해 사례 증가할 것으로 예상
- 랜섬웨어 서비스 모델 (RaaS)을 기반으로 한 랜섬웨어 등장으로
  초보자도 손쉽게 시스템 공격에 악용할 것으로 예상
- Lockbit3는 Lockbit 4.0 출시하여 관련 피해 증가할 것으로 예상

목차

2024 악성코드 분석리포트 모아보기

24 01 — WinRAR 원격코드 실행 취약점 — 리포트 확인하기
전 세계 약 5억 명이 사용하는 압축 프로그램에서 취약점 발견,
CVSS(공통 취약점 등급 시스템) 위험도 최고점 10점 중 7.8점 평가

24 01 — BiBi 와이퍼 악성코드 — 리포트 확인하기
이스라엘 공격 목적으로 친팔레스타인 단체에서 개발한
인프라 파괴 목적의 악성코드

24 07 — 와이퍼 악성코드 — 리포트 확인하기
CrowdStrike의 소프트웨어 장애 사건을 이용하여
보안 소프트웨어 업데이트 파일로 사칭

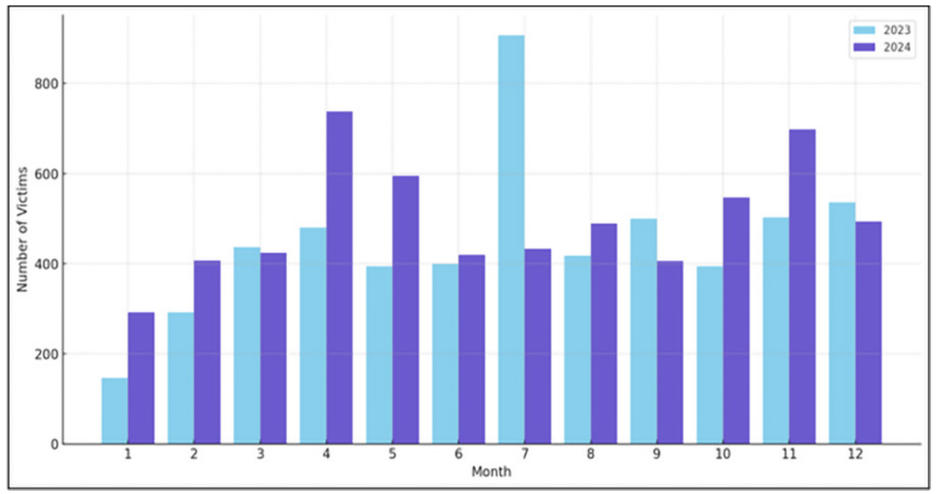
24 09 — "EDR 킬러" BYOVD 공격 — 리포트 확인하기
허가받은 서명이 적용된 정상 드라이버로 위장,
시스템 권한 실행하여 탐지 및 차단 불가능

24 10 — HexaLocker 랜섬웨어 — 리포트 확인하기
국내 대기업도 계정, 소스코드 유출피해
LAPSUS$ 그룹의 자체개발한 HexaLocker 랜섬웨어

24 12 — 악성코드 로더 'Bumblebee' — 리포트 확인하기
Conti, Diavol 등 랜섬웨어 유포에 악용,
유로폴 국제수사 후 사라졌다 재등장

〈2024년 랜섬웨어 공격 동향〉

1. 통계와 주요 지표



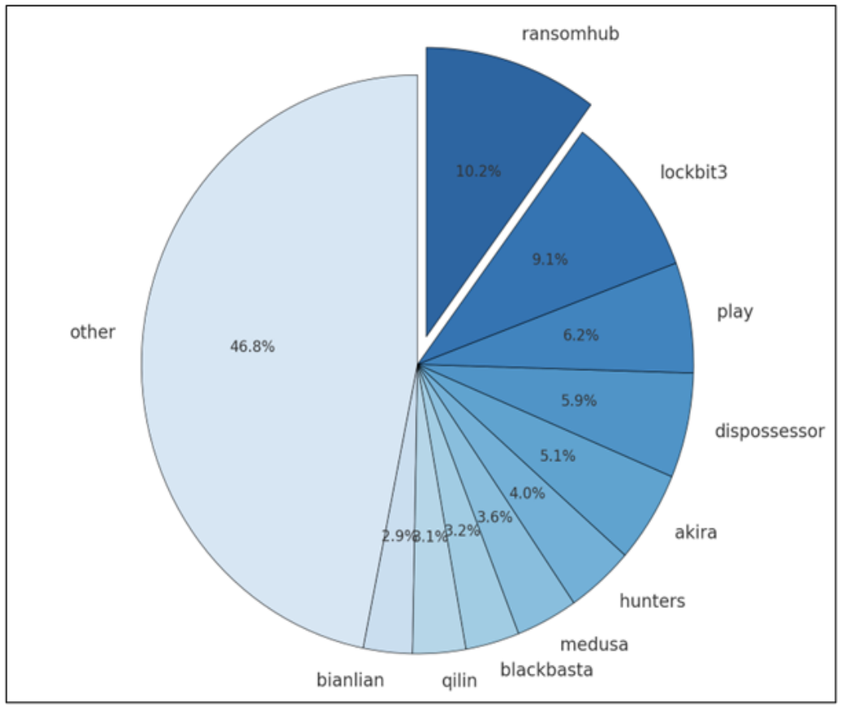
[그림 1] Aggregate Victim Count (소만사 제작)

2024년 랜섬웨어로 인한 데이터 유출 건수는 전세계 최소 5,943건으로 집계됐다.(2024년 12월 19일 기준) [01]
이는 2023년에 비해 11.37% 증가한 수치이다.

NCA, FBI, Europol 등 주요 국제 수사 기관이 랜섬웨어 조직에 대응하였으나,
랜섬웨어 조직은 끊임없이 진화하며 지속적인 위협을 가하고 있다.

01 https://www.ransomware.live/

1.1 2024년 랜섬웨어 Top 10

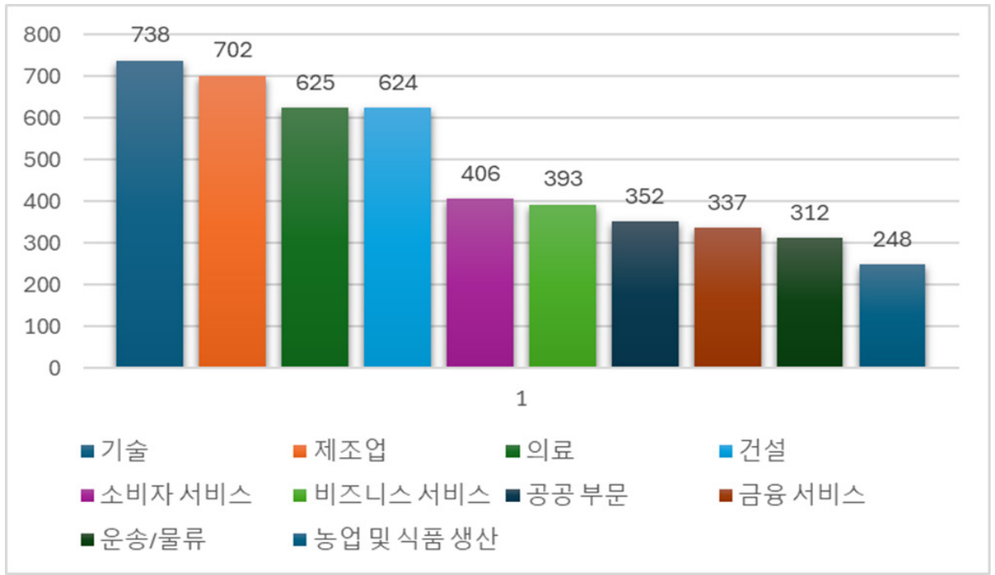


[그림 2] 2024's Top 10 Ransomware

2024년 주요 10대 랜섬웨어가 입힌 피해는 전체 피해량의 53%를 차지했다.

그 중 **Ransomhub, LockBit3, Play 랜섬웨어** 그룹이 전체 피해량의 25%를 차지하며 영향력을 보였다.
특히 Play 랜섬웨어는 VMWare ESXi 환경을 겨냥한 Linux 버전을 출시하며 피해 대상을 확대했다.

LockBit3는 LockBit4.0을 출시하며 2025년에도 지속적인 활동을 예고했다.



[그림 3] 산업별 데이터 유출 상위 10 (소만사 제작)

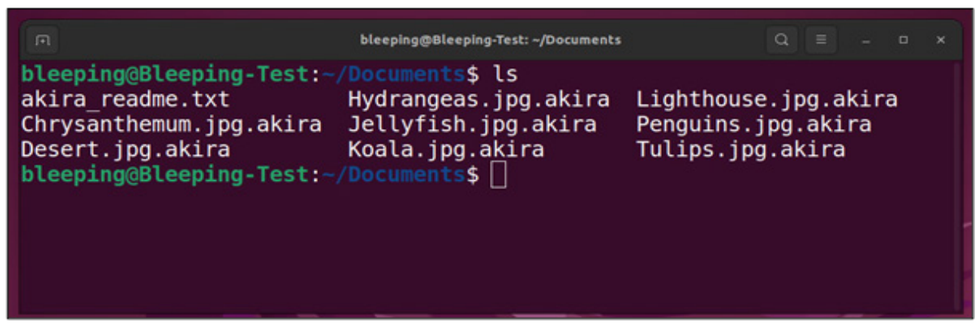
2024년 랜섬웨어 산업별 공격 동향 분석 결과,
랜섬웨어 공격의 주요 타깃이 된 산업은 **기술, 제조업, 헬스케어, 건설업**인 것으로 나타났다.

2. 주요 공격 동향

2024년, LockBit, RansomHub, Play 등 주요 랜섬웨어 공격 그룹은 전 세계적으로
심각한 경제적 손실을 입혔다.

특히, VMware ESXi 서버와 리눅스 시스템을 겨냥한 공격이 증가했으며
Ransomware-as-a-Service(RaaS) 모델의 확산으로 비전문 공격자의 참여도 늘고 있다.

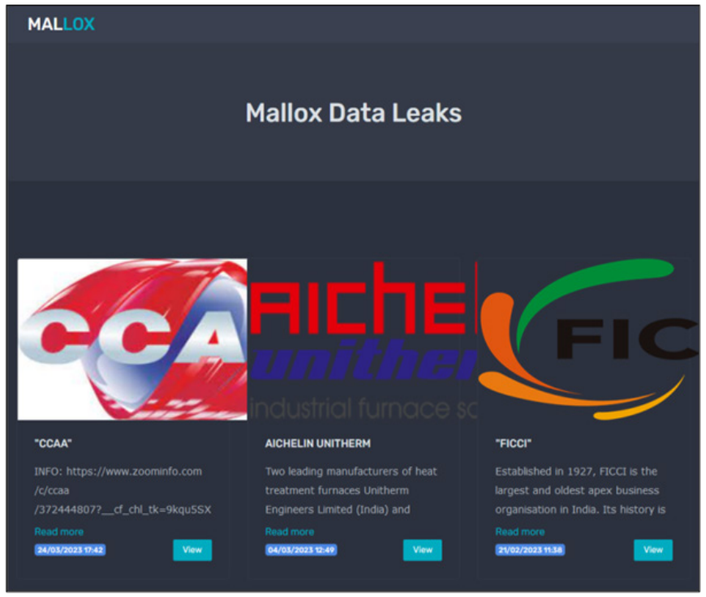
2.1. 가상화 환경과 리눅스 시스템을 노린 공격 증가



[그림 4] Files encrypted by Akira on a Linux server (출처: bleepingcomputer)

Akira, BlackBasta, 그리고 **Play 랜섬웨어 그룹**이
VMware ESXi 서버를 표적으로 한 공격을 감행했으며,
특히 Play 랜섬웨어는 새로운 리눅스 변종을 통해 서버 환경을 대상으로
더욱 정교한 위협을 가하고 있다. 이들은 가상화 환경의 보안 취약점을 악용해
데이터를 암호화하고 탈취한 뒤 금전적 요구를 제시하는 방식으로 공격을 수행한다.

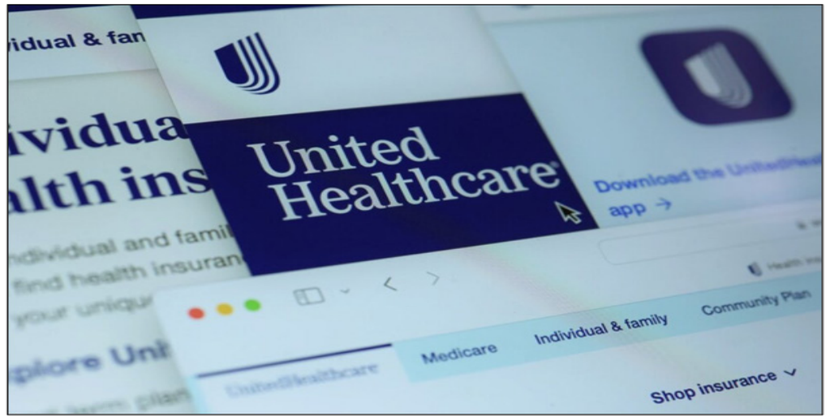
VMware ESXi 서버는 대기업 및 클라우드 서비스 제공업체에서 널리 사용되기 때문에
이러한 공격은 광범위한 피해를 초래하고 있다.
후술하겠지만 VMWare ESXi 취약점 (CVE-2024-37085)이 발견된 이후
아키라(Akira)와 블랙바스타(BlackBasta), 블랙바이트(Black Byte) 등 다수의 해킹 그룹이
해당 취약점을 적극 악용하여 공격을 수행했다.



[그림 5] Mallox Data Leaks site (출처: checkmal)

Mallox 랜섬웨어는 리눅스 시스템을 공격하도록 업데이트 되었으며
이는 2023년 말 출시된 RaaS(서비스형 랜섬웨어) 크립티나의 유출된 소스코드를 기반으로 제작되었다.
2024년 2월 해킹 포럼에 소스코드가 공개된 이후,
공격자들은 이를 활용해 **새로운 변종 'Mallox Linux 1.0'**을 개발하였다.

2.2. 의료 기관 대상 공격 증가



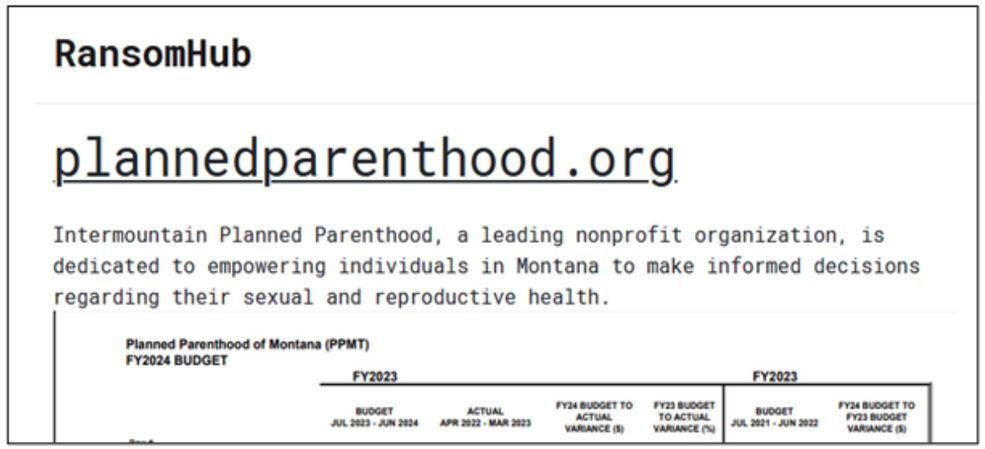
[그림 6] 체인지 헬스케어 (출처: https://krdc.tistory.com)

2024년에는 **의료 기관을 대상으로 한 랜섬웨어** 공격이
전 세계적으로 증가하며 심각한 피해를 초래했다.

2024년 2월, 미국 최대 의료 청구 처리업체인 **체인지 헬스케어(Change Healthcare)**는
랜섬웨어 공격을 받아 청구 시스템이 마비되고 환자 정보가 유출되는 등
미국 전역의 의료 서비스에 큰 혼란을 야기했다.

미국의 **Bayhealth는 리시다(Rhysida) 랜섬웨어**에 의해 시스템이 암호화되었으며,
공격자는 데이터를 공개하겠다는 협박과 함께 몸값을 요구했다.

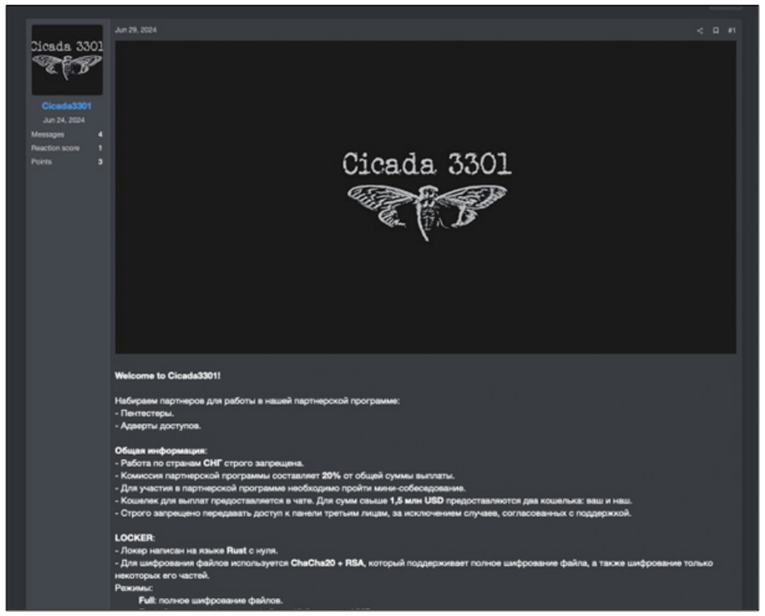
LockBit 랜섬웨어가 뉴저지의 **Capital Health**를 대상으로 사이버 공격을 수행했다.
LockBit은 데이터를 암호화하지 않았으나, 약 7TB의 의료 데이터를 탈취했다고 주장하며
이를 통해 250,000달러의 가치를 가진 정보를 확보했다고 밝혔다.



[그림 7] RansomHub의 유출 사이트에 등록된 자료 (출처: Malwarebytes)

의료 비영리 단체인 Planned Parenthood도 유사한 공격을 당해 데이터 유출 피해를 입었다.
유출 사이트의 목록에는 금융 정보, 법원 서류, 보험 증서 등의 내용이 게시됐다.
비영리 의료 서비스 제공업체인 위스콘신 중남부 그룹 건강 협동조합(GHC-SCW) 또한
랜섬웨어 갱단에 공격을 받아 50만 명 이상의 개인 및 의료 자료가 담긴 문서가 탈취됐다.

2.3. 새로운 랜섬웨어 서비스(RaaS) 그룹 등장

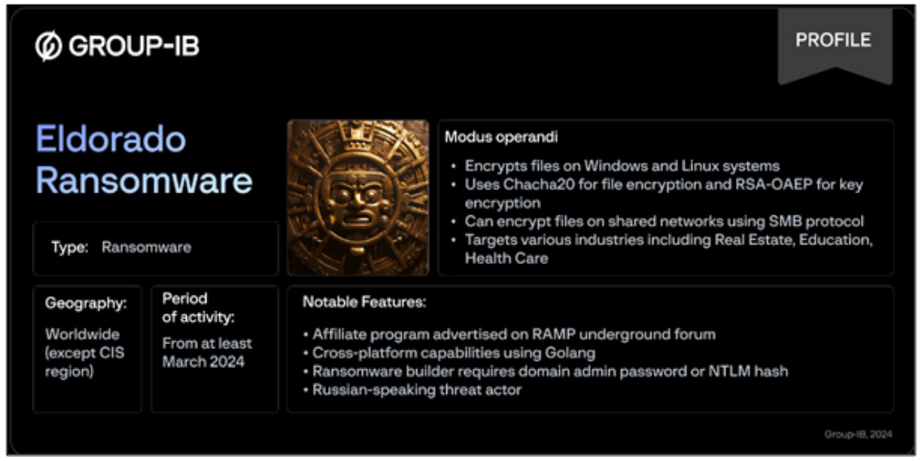


[그림 8] Cicada3301 랜섬웨어 그룹 (출처: truesec)

2024년, **Cicada3301**이라는 새로운 랜섬웨어 그룹이 등장하며[02],
Rust 언어로 개발된 랜섬웨어를 통해 VMware ESXi, Windows, Linux 환경을 공격 대상으로 삼았다.
이 그룹은 이중 협박 플랫폼(랜섬웨어와 데이터 유출 사이트)을 제공한다.
특히 가상 머신 종료와 스냅샷 제거 명령을 포함한 공격을 수행하여
가상화 된 인프라에 큰 영향을 미칠 수 있다.

Cicada3301은 ALPHV/BlackCat과 유사한 코드를 사용하며,
Rust 기반 개발, ChaCha20 암호화 방식, 동일한 파일명 규칙 등을 공유한다.
이러한 특징은 Cicada3301이 기존 랜섬웨어 생태계에서 빠르게 존재감을 드러내는 요인으로 작용하고 있다.

02 https://www.truesec.com/hub/blog/dissecting-the-cicada



[그림 9] Eldorado 랜섬웨어 그룹 (출처: group-ib)

Eldorado 랜섬웨어[03]는 Ransomware-as-a-Service(RaaS) 모델을 기반으로 운영되며,
크로스플랫폼 기능을 위해 Golang으로 개발되었다.
이 랜섬웨어는 ChaCha20 과 RSA-OAEP를 사용해 파일과 키를 암호화하며
SMB 프로토콜을 통해 네트워크 파일까지 암호화할 수 있다.

2024년 3월, RAMP 포럼에서 활동을 시작한 **Eldorado**는 Windows와 Linux 환경을 지원하며
관리자 자격 증명과 네트워크 정보를 기반으로 맞춤형 랜섬웨어를 제작한다.
기존 빌더 소스에 의존하지 않고 자체 기술로 개발된 이 랜섬웨어는 정교한 암호화와
맞춤화 옵션으로 랜섬웨어 생태계에서 빠르게 주목받고 있다.

03 https://www.group-ib.com/blog/eldorado-ransomware

2.4. 2024년 랜섬웨어 공격 기법

랜섬웨어 공격은 더욱 정교한 침투 기술과 다양해진 전략으로
전 세계 조직에 심각한 위협을 가하고 있다. 보안 솔루션의 무력화, 네트워크 침투, 사용자 신뢰 악용 등
다양한 방식이 활용되며, 랜섬웨어 생태계는 지속적으로 고도화되고 있다.
최신 피싱 기법, BYOVD 기법, ESXi 인증 우회 취약점 악용 등은
공격자들에게 효과적인 도구로 자리 잡으며, 랜섬웨어 공격의 정교함과 파괴력을 강화하였다.

2.4.1. 최신 피싱 공격 기법

[그림 10] Black Basta Ransomware (출처: socradar.io)

피싱 공격은 초기 접근에 가장 널리 사용되는 기법으로 더욱 정교하고 다양한 방식으로 발전하고 있다.
Black Basta 랜섬웨어 그룹이 **Microsoft Teams** 채팅에서
악성 QR 코드를 이용해 초기 접근을 시도하는 사례가 보고되었다.
이 공격은 사용자를 속여 QR 코드를 스캔하도록 유도하고
원격 모니터링 도구를 설치해 자격 증명을 탈취하거나 시스템에 접근을 시도한다.

2024년 4월, **Phorpiex 봇넷**이 수백만 건의 피싱 이메일을 배포하며
LockBit Black 랜섬웨어를 유포한 사례가 보고되었다.
이 이메일에는 ZIP 파일이 첨부되어 있었으며 실행 파일을 포함하고 있었다.
사용자가 이를 실행하면 LockBit Black 랜섬웨어가 설치되는 방식이다.
이처럼 이메일 첨부 파일로 랜섬웨어를 직접 유포하는 경우도 있지만,
IcedID, Emotet, Bumblebee[04]와 같은 로더를 이용해 랜섬웨어를 배포하는 방식이 일반적으로 사용된다.

04 https://www.somansa.com/wp-content/uploads/2025/01/Bumblebee_2501-1.pdf

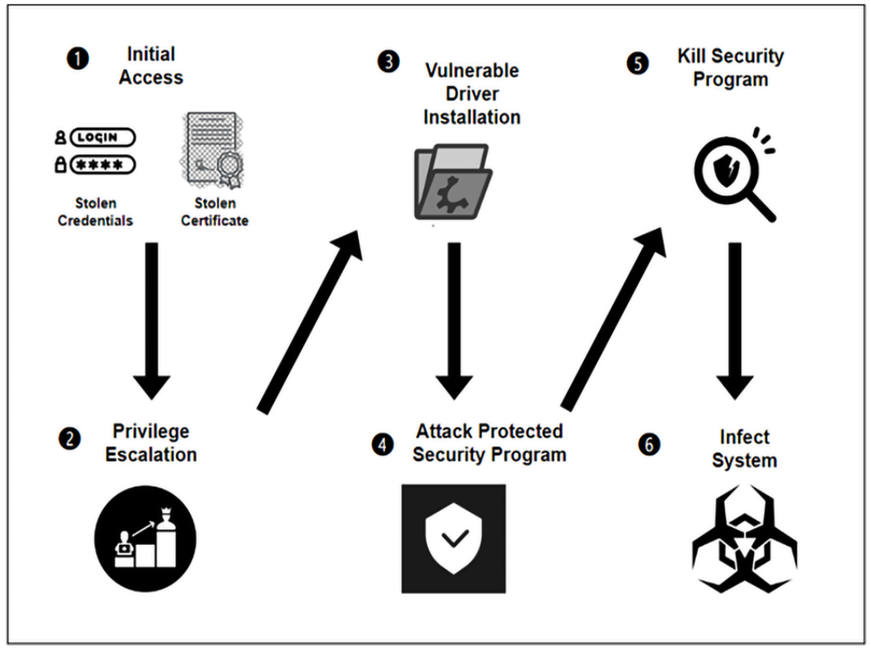
2.4.2. “EDR Killer” BYOVD 기법

Bring-Your-Own-Vulnerable-Driver(BYOVD)[05]는 공격자가 취약한 드라이버를 악용하여
시스템 권한을 상승시키고 보안 솔루션을 무력화하는 고급 기법을 사용한다.
2024년 초부터 BYOVD 공격 사례가 급증하며 발생률이 4배나 증가했다.
취약한 드라이버를 악용해 시스템에 접근하고 제어하며
특히 랜섬웨어 공격 시나리오에서 선호되고 있다.
Kasseika, Ransomhub, Cuba, GhostLocker, INC, Rhysida, Medusa와 같은
악명 높은 그룹들에 의한 공격의 중심이 되었다.

[그림 11] Kasseika Ransomware (출처: gbhackers.com)

2024년 1월 23일, 트렌드마이크로 연구원들이 **Kasseika** 랜섬웨어가
BYOVD (Bring-Your-Own-Vulnerable-Driver) 기법을 활용한 사례를 보고했다.
Kasseika는 Martini 드라이버를 악용하여 피해 시스템의 안티바이러스 관련 프로세스를 종료시키고
보안 솔루션을 무력화한 뒤 랜섬웨어를 배포했다.
2024년, **Ransomhub 랜섬웨어** 그룹은 BYOVD 기법을 활용한
새로운 악성코드 **‘EDRKillShifter’**를 배포하여 엔드포인트 탐지 및 대응(EDR) 소프트웨어 무력화를 시도했다.
8월 14일, Sophos는 이 도구가 Ransomhub 공격자들에 의해
엔드포인트 보안 솔루션을 비활성화하는 데 사용되었음을 발견하고 이를 발표하였다.

05 https://www.somansa.com/wp-content/uploads/2024/10/BYOVD_202409.pdf



[그림 12] 보안 제품을 무력화하는 BYOVD 공격 흐름

① Initial Access
- 초기 침투를 위해 계정 정보/인증서 탈취 등을 통해 시스템에 침입한다.

② Privilege Escalation
- BYOVD 공격을 수행하기 위해 드라이버를 설치할 수 있는 권한을 확보한다.

③ Vulnerable Driver Installation
- 권한이 확보된 후 BYOVD 공격에 사용할 드라이버를 시스템에 설치한다.

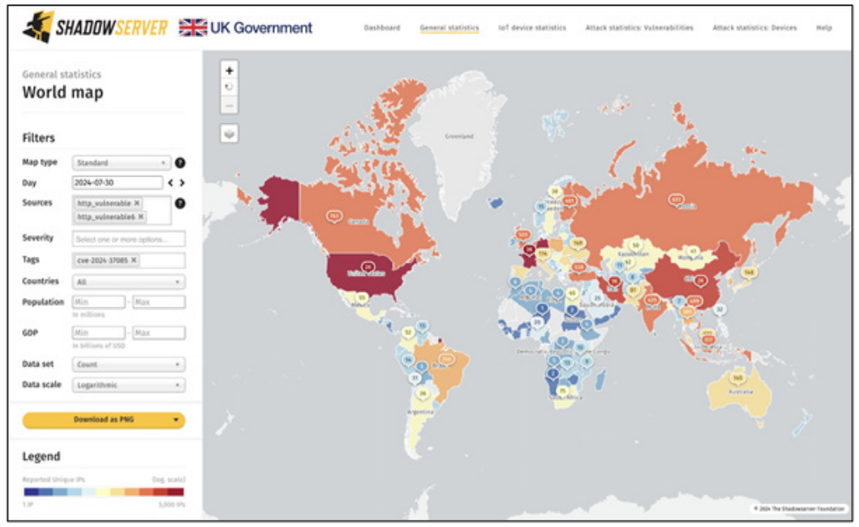
④ Attack Protected Security Program
- 시스템의 보호를 담당하는 주요 보안 제품을 무력화하기 위해 공격을 수행한다.

⑤ Kill Security Program
- 주요 보안 제품은 BYOVD 공격에 의해 무력화되며, 시스템의 보호는 무력화된다.

⑥ Infect System
- 보안 제품이 무력화되어 시스템은 공격자에게 장악당한다.

2.4.3. VMWare ESXi 인증 우회 취약점(CVE-2024-37085)

가상화 환경을 표적으로 한 피해가 급증하고 있는 추세이다.
특히, 리눅스 서버를 겨냥하는 랜섬웨어가 증가하는 동향과 함께
VMware ESXi의 취약점을 악용한 공격 기법도 등장하고 있다.



[그림 13] 20,000 internet-exposed VMware ESXi instances (출처: X(구:트위터))

올해 8월, Microsoft는 여러 랜섬웨어 갱단이
최근 패치된 VMWare ESXi 취약점 (CVE-2024-37085)를 악용하고 있다고 경고했다.

Storm-0506, Storm-1175, Octo Tempest, Manatee Tempest와 같은 랜섬웨어 위협 그룹에서
Akira, Black Basta, Babuk, Lockbit, Kuiper와 같은 ESXi 암호화기를 지원하거나 판매했다.
마이크로소프트 Incident Response(Microsoft IR) 조사에 따르면
ESXi 하이퍼바이저를 대상으로 하거나 영향을 미친 사건의 수가
지난 3년간 두 배 이상 증가한 것으로 나타났다.

〈2025년 랜섬웨어 전망과 대응 방안〉

1. 2025년 전망

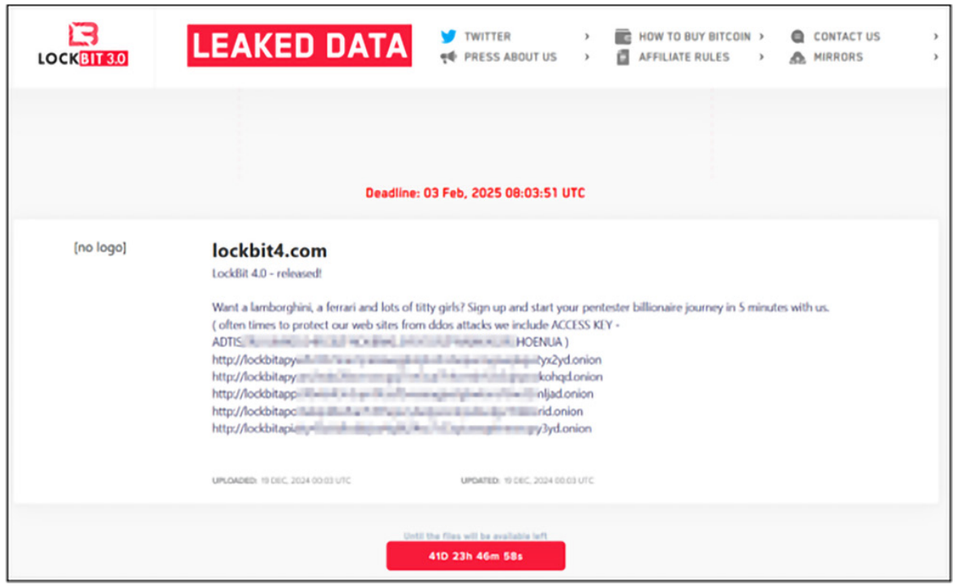
1.1. macOS 공격, 크로스플랫폼 언어 활용 등 공격기법 진화

[그림 14] macOS Ransomware (출처: SentinelOne)

2025년에는 랜섬웨어 수법이 더욱 진화하며 다양한 운영체제와
환경을 아우르는 공격이 지속적으로 증가할 것으로 예상된다.
2024년에 등장한 **NotLockBit과 같은 macOS 지원 랜섬웨어**는
공격 범위가 전통적인 Windows 환경을 넘어 확대되고 있음을 보여주었다.
Rust와 Golang 같은 크로스플랫폼 언어를 활용한 멀티플랫폼 랜섬웨어는
2025년에도 주요 공격 도구로 자리 잡을 가능성이 크다.

특히, 가상화 플랫폼인 VMware ESXi와 Linux 환경을 겨냥한 공격이 증가할 것으로 보이며
랜섬웨어 개발자들은 기존의 운영체제뿐 아니라 클라우드 기반 시스템, IoT 장치, macOS 등
상대적으로 덜 공격받았던 플랫폼으로까지 공격 대상을 확장할 것으로 예상된다.
이러한 흐름은 기술적으로 정교한 암호화 방식과 새로운 침투 전략을 통해
공격이 한층 더 고도화될 것을 시사한다.

1.2. 확대되는 랜섬웨어 서비스 모델(RaaS)[06] 생태계



[그림 15] Lockbit4.com 출시

랜섬웨어 서비스 모델은 랜섬웨어 생태계의 중심으로 자리 잡으며
숙련된 제휴사를 모집하는 조직적인 파트너십을 통해 대규모 공격을 가능하게 하고 있다.
특히, LockBit은 **2024년 12월 LockBit 4.0 출시를 발표**하며
2025년에도 활발한 활동을 이어갈 것으로 보인다.

이처럼 기존 랜섬웨어 변종의 지속적인 등장과 새로운 RaaS 그룹의 출현은
RaaS 모델의 확산 가능성을 더욱 높이고 있다.
RaaS는 기술적 역량이 부족한 공격자들에게도 랜섬웨어를 손쉽게 배포할 수 있는 플랫폼을 제공하며
이를 통해 더욱 정교하고 파괴적인 공격을 가능하게 한다.

RaaS 모델의 발전과 LockBit 4.0, Eldorado와 같은 그룹의 등장은
랜섬웨어 위협이 빠르게 진화하고 있음을 보여주는 대표적인 사례이다.
이러한 변화 속에서 보안을 강화하고 선제적인 대응 방안을 마련하는 것이 그 어느 때보다 중요해 보인다.

06 Ransomware-as-a-Service

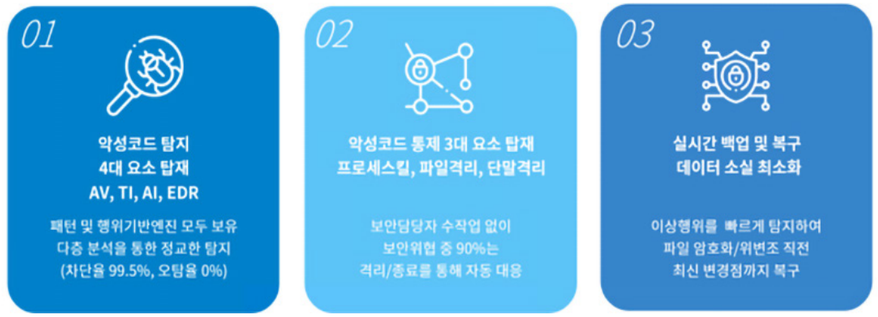
2. 랜섬웨어 대응 방안

2.1. 실시간 백업을 통한 조직 내 자산 보호

실시간 백업은 데이터 손실을 방지하고, 조직의 자산을 보호하는 중요한 보안 전략 중 하나이며
랜섬웨어에 의해 손상된 조직의 자산을 보호하는 데 중요한 역할을 한다.
이를 통해 조직은 데이터 손실을 방지하고, 업무 연속성을 유지하며 빠르고 효율적인 복구를 수행할 수 있다.
보안 제품이 탐지하지 못하는 신종 또는 변종 랜섬웨어에 대비하기 위한
실시간 백업은 데이터를 안전하게 보호하고 복구할 수 있는 최후의 보루 역할을 수행한다.

2023년 8월 21일 국가정보원에서 제정한 '랜섬웨어 대응제품 보안요구사항'은
사용자 데이터를 보호하는 기능을 제공해야 하며,
사용자 데이터를 보호하는 방법 중의 하나로 실시간 백업을 명시하고 있다.

3. Privacy-i EDR의 랜섬웨어 대응

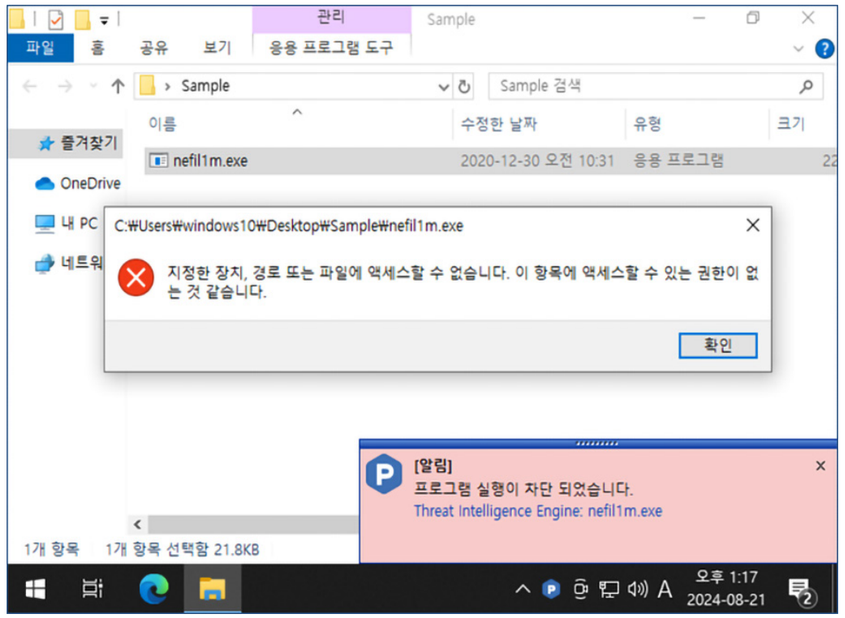


[그림 16] Privacy-i EDR 차별화 기능

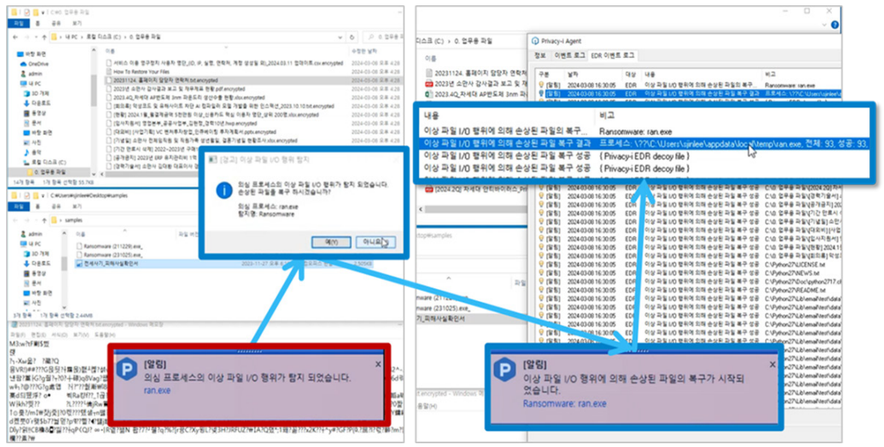
Privacy-i EDR은 알려진 랜섬웨어 뿐만 아니라 **신종 또는 변종 랜섬웨어에 대응**하기 위하여 **다계층 보안 기능**을 제공하고 있다. 랜섬웨어 초기 침투 시, **정적 분석 엔진**은 순차적으로 안티바이러스 엔진, 위협 인텔리전스, AI엔진을 통해 악성코드를 탐지한다.

정적 분석 엔진으로 탐지되지 않은 신종 또는 변종 랜섬웨어는 엔드포인트에서 실행되어 조직 내 자산을 암호화를 시작한다.

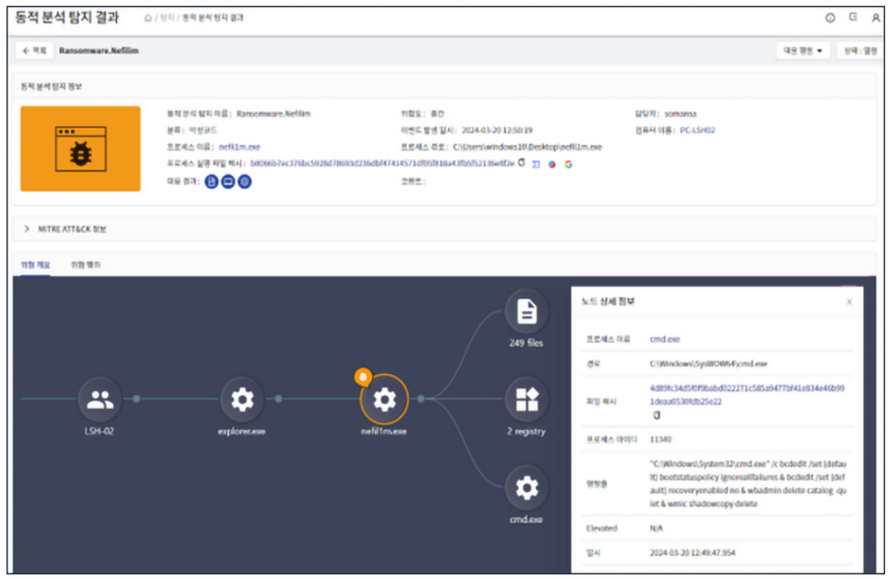
동적 분석 엔진은 이러한 암호화 행위를 탐지하고 **실시간 백업**을 통해 **데이터 유실을 방지**하며 무분별한 데이터 암호화 행위를 기반으로 신종 또는 변종 랜섬웨어를 탐지하고 랜섬웨어 프로세스를 강제 종료하여 데이터 암호화를 중단시킨다.



[그림 17] Privacy-i EDR 정적 분석 엔진에서 탐지 된 랜섬웨어 실행 차단 화면



[그림 18] Privacy-i EDR 랜섬웨어 탐지 후 복구 완료 화면



[그림 19] Privacy-i EDR 랜섬웨어 로그

대응

1. Privacy-i EDR과 같은 EDR 제품을 통해 취약점 실행을 행위 기반으로 차단
2. 주요 데이터는 주기적인 백업을 통해 시스템 파괴 시에도 복구가 가능하도록 대비
3. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단
4. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션
5. PC 취약점을 주기적으로 점검, 보완
6. 신뢰할 수 없는 메일의 첨부파일 실행 금지
7. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결 차단
8. OS나 어플리케이션은 최신 형상 유지

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오